А. Е. Александрович, В. О. Чуканов

ИССЛЕДОВАНИЕ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ БОЛЬШИХ ИНФОРМАЦИОННЫХ СИСТЕМ ОТВЕТСТВЕННОГО ЦЕЛЕВОГО НАЗНАЧЕНИЯ

Вопросы функциональной безопасности информационных систем (ИС) ответственного целевого назначения решаются на всех этапах их проектирования. Немалую роль в обеспечении функциональной безопасности ИС играет обеспечение их надежности и функциональной безотказности. Обеспечение заданного уровня отказоустойчивости ИС трактуется как защита ИС от вредоносного воздействия случайных факторов их функционирования. К числу случайных факторов, как правило, относят аппаратные неисправности, ошибки программного обеспечения и ошибочные действия пользователя (администратора, оператора).

Как отмечается в [1], современные ИС имеют ряд особенностей с точки зрения оценки их надежности. Во-первых, они зачастую имеют распределенный характер и включают в себя набор станций, взаимодействующих друг с другом по каналам телекоммуникации или сетевой связи. Во-вторых, организация их эксплуатационной поддержки также усложнилась: часть служб может обеспечиваться в локальном режиме, а часть — централизованно, например служба пополнения локального комплекта ЗИП из главного центра поддержки оборудования. В-третьих, при расчете надежности таких ИС бывает необходимо учитывать разнообразный набор критериев для различных функциональных компонентов системы. Например, для рабочего сервера в качестве критерия может выбираться обычный коэффициент готовности или среднее время наработки на отказ, для канала связи — вероятность безошибочной информационной передачи или вероятность передачи с заданным порогом качества, для службы ЗИП — среднее время обслуживания заявки на пополнение или коэффициент готовности ЗИП. Анализ качества и надежности функционирования всей системы в целом предполагает использование либо стандартных критериев типа стационарного коэффициента готовности, либо критериев, связанных с особенностями ее целевого назначения. В качестве таких дополнительных критериев можно назвать процент неудавшихся/успешных сеансов связи (для коммуникационных систем), процент выполненных заявок (для систем массового обслуживания пользователей) и т. д.

В качестве примера рассмотрим информационную систему, предназначенную для мониторинга российских атомных электростанций [2]. Система (получившая название «система передачи данных» — СПД) имеет звездообразную структуру, в центре которой находится управляющая станция (станция Кризисного центра), а периферийными узлами являются серверные станции отдельных АЭС. Оборудование каждой станции включает в себя несколько рабочих серверов,

обеспечивающих управление коммуникацией, контроль технологических параметров, сбор данных и т. д. Связь между центральной и периферийными станциями системы осуществляется по спутниковому каналу связи. Резервным каналом связи является сетевой канал наземной связи.

Анализ функциональной безопасности и надежности такой сложной распределенной системы производился на различных уровнях ее представления:

а) на уровне отдельного рабочего сервера,

б) на уровне оборудования отдельной станции,

в) на уровне отдельного коммуникационного звена «центральная станция — периферийная станция», получившего название типового направления связи (ТНС) СПД,

г) на уровне всей системы в целом.

На нижних уровнях представления системы использовались аналитические методы расчета надежности; на верхних уровнях (начиная с третьего уровня ТНС СПД) наряду с аналитическими моделями был разработан ряд имитационных моделей надежности, реализованных на языке GPSS в среде GPSS World. Как известно, имитационные модели позволяют учесть произвольные факторы функционирования системы и получить оценки разной степени точности при наличии достоверных исходных данных.

В рамках данной работы созданы аналитические модели надежности:

1) рабочего сервера системы,

2) аппаратуры одной станции,

3) ТНС с учетом типов отказов и режимов восстановления серверов,

4) ТНС с учетом резервирования рабочих серверов и службы общего ЗИП,

5) функционирования служб локального и общего ЗИП,

6) всей системы с учетом пространственной конфигурации службы ЗИП,

7) всей системы с учетом типов отказов и режимов восстановления системы.

В зависимости от конкретной задачи анализа (исследования) и соотношения исходных параметров для исследования выбирается та или иная модель надежности системы и ее компонентов.

Например, модель 3 описывается формулой:

$$K_{ГС} = (1-(\frac{t_n}{t_n+N\lambda(k+n)})^m)\sum_{i=0}^{i=k} C_i^{n+k} K_{Г0}{}^{k+n-i}(1-K_{Г0})^i,$$

где $К_{ГС}$ — коэффициент готовности станции, $Т_0$ — средняя наработка сервера на отказ, $Т_В$ — среднее время локального восстановления сервера, $Т_Д$ — среднее время дистанционного восстановления сервера, С — доля «сложных» отказов, требующих дистанционного или длительного восстановления (например, при вызове специалистов централизованной службы). Под «сложным» отказом может пониматься и случай, при котором локальный резерв исчерпан и при отказе сервера приходится ожидать пополнения запасов оборудования (доставки). Приведена формула, соответствующая случаю, когда все рабочие серверы станции объединены в один информационно-коммуникационный сервер.

Модель 4 описывается следующей формулой:

$$K_C = (\sum_{i=0}^{\frac{Nz}{Z}} C_m^i K_{Г0}{}^{m-i}\cdot(1-K_{Г0})^i)^Z, K_{Г0} = \frac{t}{t+\frac{t_B}{Z}},$$

где N — число станций в системе, k — число резервных серверов станции, n — число рабочих серверов станции, $t_п$ — время пополнения (восстановления) общего ЗИП, $К_{Г0}$ — коэффициент готовности рабочего сервера системы, $К_{ГС}$ — коэффициент готовности станции.

Модель 6 описывается формулой:

$$K_{ГС} = \frac{T_0}{T_0 + T_B(1-C) + T_Д C},$$

где t — наработка на отказ одного сервера, t_B — среднее время восстановления сервера, Z — число региональных центров обслуживания (ЗИП), $К_{Г0}$ — коэффициент готовности одного сервера, $К_С$ — коэффициент готовности всей системы.

Рис. 1. График зависимости готовности системы от числа региональных центров обслуживания

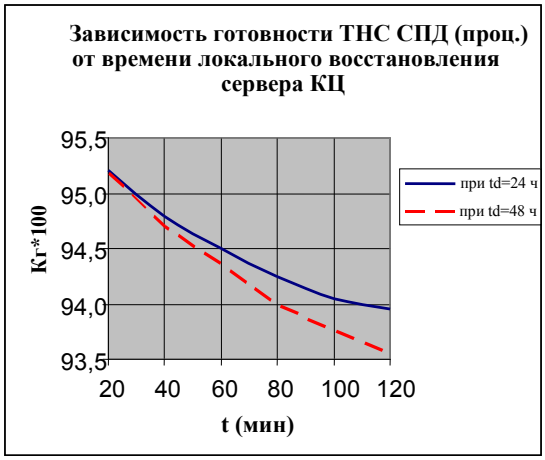

Рис. 2. График зависимости готовности ТНС СПД от времени локального восстановления сервера КЦ

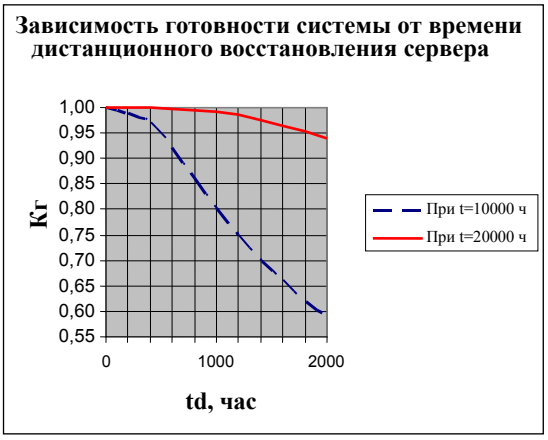

Рис. 3. График зависимости готовности системы от времени дистанционного восстановления сервера

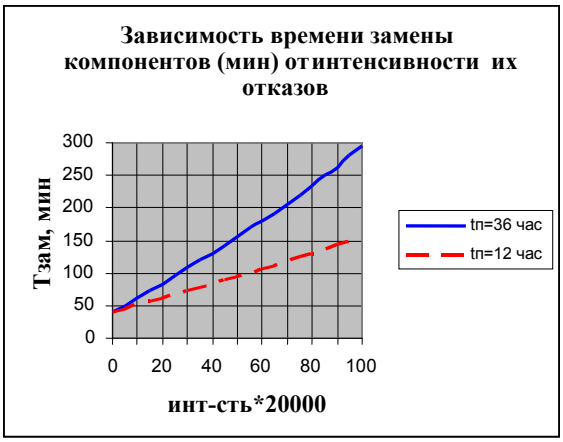

*Рис. 4. График зависимости времени восстановления компонентов от интенсивности их отказов (*20000 час).*

Аналитический характер подобных моделей позволяет легко использовать их для исследования и получения рациональных решений. Например, на рисунке 1 представлен график зависимости готовности системы от числа Z региональных центров обслуживания (восстановления отказавших компонентов), полученный с помощью модели 6. На рисунке 2 представлен график зависимости готовности ТНС СПД от времени локального восстановления сервера центральной станции, построенный для двух значений времени дистанционного восстановления сервера (td): td = 24 часа и td = 48 часов. График получен на основе модели 3. Напомним, что время дистанционного

восстановления сервера можно трактовать как время пополнения соответствующего комплекта ЗИП (время заказа, доставки и инсталляции).

На рисунке 3 представлен график зависимости готовности всей системы от времени дистанционного восстановления серверов (модель 4). График построен для двух значений наработки на отказ сервера системы: t = 10 тыс. часов и t = 20 тыс. часов.

На рисунке 4 приведен график зависимости времени восстановления компонентов системы из локального ЗИП (модель 5), построенный при двух значениях времени пополнения локального ЗИП (tп): tп = 36 часов и tп = 12 часов.

Заключение

В результате проведенных работ создан ряд аналитических моделей надежности безопасной системы СПД и ее компонентов. Все разработанные аналитические модели реализованы в среде Delphi с использованием классов и объектов для представления и отображения различных системных компонентов. С помощью созданных программ были произведены различные исследования надежности и функциональной безопасности системы с оперативным представлением результатов в графическом виде. Результаты исследований были использованы при проектировании и обеспечении функциональной безопасности системы СПД, предназначенной для мониторинга российских АЭС.

СПИСОК ЛИТЕРАТУРЫ:

1. *Александрович А. Е., Бородакий Ю. В., Чуканов В. О.* Проектирование высоконадежных информационно вычислительных систем. М.: Радио и связь, 2004. — 144 с.
2. *Чуканов В. О.* Надежность программного обеспечения и аппаратных средств систем передачи данных атомных электростанций. М.: МИФИ, 2008. — 168 с.